Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 :
CIA-RDP89G00643R000300030005-6

TRANSMITTAL SLIP	DATE

TO:

ROOM NO.	BUILDING

REMARKS:

EXA _____ 14 SEP 1987

14 SEP 1987

ADDA _____

DDA _____ 15 SEP 1987

EXA _____ Urge OS to include

DDA/Registry 15 SEP 1987 OIR, pls.

done

sd

9/15/87

FROM:

ROOM NO.	BUILDING	EXTENSION

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 :
CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

OFFICE OF THE DIRECTOR

Office of Security

TO: Deputy Director for Administration

SUBJECT: FBI Briefing on Computer Crime

Bill:

As you can see from the attached, I have arranged for FBI Agent Lane to brief us on computer crime. I have invited D/OIT, C/CI Staff and C/IMS. You are of course also welcomed.

STAT

Atts

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

11 SEP 1987

MEMORANDUM FOR: Director of Information Technology, DA
Chief, Information Management Staff, DO
Chief, Counterintelligence Staff, DO

STAT FROM: [redacted]
Director of Security

SUBJECT: FBI Briefing on Computer Crime

1. I have made arrangements for Mr. George Lane, who is an FBI agent, to brief us on gathering evidence in computer crime. Bill Donnelly heard Mr. Lane's briefing at a recent National Telecommunications Information Systems Security Committee (NTISSC) meeting and suggested the message was one that should be shared. Mr. Lane will be speaking to us on
STAT 22 September at 1000 hours in [redacted] You and two or three members of your staff are invited to join me.

2. Attached are two documents relevant to this topic.

STAT [redacted]

Attachments

cc: DDA

10-10

OS 7 8036

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

EVIDENTIARY ASPECTS OF COMPUTER CRIME

BY

Stephen C. Gross

Crime in Commerce III: ~~Management~~ Information Systems
ForS 234
December 18, 1986

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

TABLE OF CONTENTS

		Page
I.	INTRODUCTION	1
II.	COMPUTER EVIDENCE CONSIDERATIONS	2
	A. Search and Seizure	2
	B. Obtaining Computer Evidence	5
	C. Computer Records and Reports as Evidence	6
	D. Storing and Caring for Evidence	8
	E. Privacy and Secrecy of Evidence	9
III.	PROSECUTION AND COMPUTER EVIDENCE	10
	A. Foundational Problems	10
	B. Evidentiary Problems with Computer Records	12
	C. Practical Recommendations	14
IV.	CONCLUSION	15
	FOOTNOTES	18
	BIBLIOGRAPHY	21

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

I. INTRODUCTION

Computers and information systems have permeated today's society to such an extent that there is virtually no sector which does not rely heavily on their use. 1/ As might be expected, computer crime has also expanded, with resulting annual losses incurred, by any measure, enormous. In fact, respondents to an American Bar Association survey of private organizations and public agencies disclosed estimated total annual losses between $145 million and $730 million, highlighting the need for more and better computer crime investigative efforts. 2/ As is true in any investigation or preparation for court trial, the use of evidence is a significant element. In fact, the most likely of the principle defense strategies that will arise in a computer-related crime case will be an attack on the admissibility of computer generated physical evidence. This paper will discuss computer evidence issues based on general law principles and sound investigative procedures, including preventive measures to be considered during all investigative and prosecutive stages. 3/

Initially, the discussion will focus on computer evidence considerations from an investigative perspective. Search and seizure issues will be discussed, as well as procedures used in obtaining computer evidence, computer records and reports as evidence, proper handling and storage of computer evidence, and computer evidence privacy and secrecy considerations. Next, we will address foundational problems encountered in computer crime cases, problems associated with admitting computer records into evidence, and, finally, some practical recommendations for the successful prosecution of computer crime cases.

It is not surprising to see attention focusing on computer crime, considering the power and leverage of computers, the dependence upon them, and their increasing role in society. 4/ Suceeding in combatting the growing threat imposed by bomputer-related crime will depend upon the knowledge and

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

computer crime evidence will be crucial to this fight.

II. COMPUTER EVIDENCE CONSIDERATIONS

A. SEARCH AND SEIZURE

As computer technology becomes more accessable, so does the liklihood of computer crime; the computer is quickly becoming "abuser friendly". 5/ Investigators seeking and executing search warrants authorizing the seizure of computers and related computerized information are generally on untested ground since complete judicial guidance is still limited in this area. 6/ They must comply with an 18th century prohibition against "unreasonable searches and seizures" while contending with 20th century electronic technology; an often formidable task. They may sometimes find themselves searching for intangible rather than the ordinary and more familiar types of evidence, such as stolen guns and stock certificates. 7/ Very little has been done to overcome obvious problems in discovery, search warrants, and subpoenas. 8/ Thus, a pandora's box of legal issues becomes available to the defense regarding computer evidence, requiring alert prosecutors to be ever mindful of this potential. Fortunately, those routine issues concerning search and seizure, such as consent, informers, entry, and searches incident to arrest generally will arise and apply much as they would in noncomputer-related cases. 9/ But, what are the necessary steps to take in conducting a successful search and in gathering computer evidence in the non-routine situations?

In general, search warrants should be obtained and used in computer-related crime cases. 10/ Regardless of technological advances, search and seizure by law enforcement officers continues to be governed by the fourth amendment to the U.S. Constitution, protecting the right of the people to be secure against unreasonable Government intrusion. This protection extends to computers and to computer processed information and requires that proper search warrants be

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

obtained prior to legitimate searches. This requirement is applied with special strictness where businesses or residences, the places where computers are most likely to be located, must be entered to perform the search. There must be a showing of probable cause and the warrant must particularly describe the place to be searched and the persons or things to be seized. Unique problems can sometimes arise concerning probable cause and particularity where computers are the search target and will comprise the evidence to be seized. 11/

It is necessary to excercise great care in preparing a search warrant in a computer crime case, due in large part to this being a technical area often new and unfamilier to judges and magistrates. The investigator should have a detailed affidavit which covers all the technical bases, yet is understandable to someone who knows very little or nothing at all about computers. 12/ The difficulties involved in such a task become apparent when one considers the enormity and complexity of the "scene of the crime"in some of the larger business computer centers. For instance, in the litigation involving Equity Funding Corporation of America, thousands of fictitious insurance policies had been created and existed somewhere within a computer memory. At the same time, that particular computer was processing hundreds of thousands of valid insurance policies. 13/

It becomes apparent that one of the first obstacles to be overcome is explaining in an affidavit that certain records being sought may be contained in sophisticated technological equipment. Fortunately, this obstacle is normally easily overcome since the investigator seeking the search warrant can simply state that the information sought may be in electronic or written form, thereby circumventing a non-meaningful description of the computerized information in its encoded form. It is more critical that the information itself be described with particularity, rather than in the form in which it may be found. Also, the storage media which contains the information should be described as concisely as the facts known will allow. 14/

Another hurdle to overcome in establishing probable cause to search is to

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

articulate the necessary facts to show that a crime has actually been committed. In doing so, it is helpful to examine the role played by the computer in the criminal activity and then detailing to the magistrate that such a crime has been committed. The mechanics of the crime should be clear and easily understood. In instances where the crime is unusual or unfamiliar, the investigator should consider using the services of a computer expert.

At this point the investigator must set forth enough facts to convince a magistrate of the probability that evidence of the crime exists at the place to be searched. The legal requirement for recent information is satisfied where the investigator can set forth reliable information that the objects sought were recently observed at the proposed search site. 15/

Although search warrants are preferable in computer-related crime cases, special mention and consideration should also be given to situations providing application of exigent circumstance exceptions to preserve evidence because of the high degree of ease with which both the instruments and fruits of the crime can rapidly destroy or alter the computer evidence. 16/ Because any power interruption will result in the loss of information stored in the computer's internal memory, valuable evidentiary data can be destroyed in the instant it takes to flip a power interruption switch. Also, a magnetic device known as a degausser can instantly erase millions of data characters from a computer tape or disc. Therefore, a "no-knock" entry is reasonable where the investigator reasonably believes that making a pre-entry announcement will result in destruction of the evidence. 17/

The "plain view" doctrine is another possibility, however, this should be used cautiously since there is a strong liklihood that defense attornies will attempt to show the lack of sophistication of most investigators in computer technology. Also, avoid reliance on "expert" informants to point out at the scene what items should be seized. They will generally be insiders and will likely be legally

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Overall, investigators should be open to using imagination and ingenuity, as well as their training, to optimize their results in computer related search and seizure situations.

B. OBTAINING COMPUTER EVIDENCE

Evidence in a computer is much more "dense" than in any other information system, in that a single computer tape can contain as much information as a shelf full of books. As an example, in the Equity Funding case alone, approximately 3,000 reels of computer tapes were potential evidence ! 19/ Ensuring that the best evidence for prosecution available at the crime scene is obtained can be both challenging and rewarding for the careful investigator..

When a search is directed towards obtaining documents, they can normally be visually identified and expert knowledge of computer technology is unneccessary. 20/ Documentation practices vary from phenomenally obsessive and complete to non-existent. Ideally, they will thoroughly describe every aspect of the computer system and list each type of output that it produces. 21/ Documents such as systems manuals, computer run books, interpreted punch cards, program documentation logs, data and program input forms, and computer printed forms are usually labeled as to their contents and should be relatively easy to recognize. The completeness and originality of these documents can be determined by careful and complete questioning of those who are most familiar with them. 22/

Recognizing and requesting program documentation is somewhat more difficult and may require knowledge of computer program concepts to understand the types and extent of documentation required, such as source and object listings, flowcharts, test data, and storage dumps. It must also be realized that program documentation is frequently obsolete relative tocurrently used versions and,

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

thus, may necessitate new computer printouts. If the investigator is unsure about what may be obtained or identified, an expert should accompany him on the search. 23/

Taking possession of other computer media materials may be more technically complex. Magnetic tapes and disks will normally have external labels, however, logs and program documentation will normally be necessary to obtain full titles and descriptions of their contents. A trusted technologist may be necessary to check a tape or disk's contents by using a compatable computer and computer program. 24/

Also, where appropriate, consideration should be given to shutting down the operation of the business being searched for a reasonable time to protect the evidence covered by the warrant and to properly sort through the computer documentation. 25/ This sorting process, performed at the scene, can serve to prevent the seizure, and thus the denial of access and use by the owner, of innocent records. The mere fact that the sorting process is time consuming will not necessarily render a wholesale seizure of records reasonable. 26/

C. COMPUTER RECORDS AND REPORTS AS EVIDENCE

Computer records may be divided into two types: (1) computer-stored, where the printout produced from computer storage is a restatement of information or data previously supplied to the computer; and (2) computer-generated, where the computer makes a computation, performs a logical operation, or analyzes the input and other stored data. In judicial proceedings, a distinction appears to be drawn between the two types. It is more difficult to get computer reports containing computer-generated records into evidence. This is probably because computer-stored records are more easily equated with ordinary business records, while computer-generated data involves the complexity of examining the creation of the generated information and the deceptively neat package in which it is displayed. 27/

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

There is no clear-cut answer as to which kind of computer output can or cannot be admissable as evidence, whether from a printer, cathode ray tube, audio response, microfilm, or speech mail. In the case of "Cotton v. John W. Eshelman & Sons, Inc, the court held that computer generated output was admissable, since "our statute was intended to bring the realities of business and professional practice into the courtroom and should not be interpreted so as to destroy its obvious usefulness". Generally, the court will apply the following rules (Business Records Exception to the Hearsay Rule) to evaluate the admissibility of computer output as evidence: (1) that the records were made in the usual course of business, and not merely for the purpose of litigation; (2) it was normal business procedure for an employee with knowledge of the act to make the record; and (3) the record was made at or near the time of the act. 28/

Another possible basis for admission of computer digital-image printouts into evidence is the "Best Evidence Rule". This rule requires that original writing or recording is necessary to prove its own contents; however, if the original is unavailable, then other relevant evidence of its contents is admissable unless the original was lost or destroyed in bad faith. 29/

During the procedure of obtaining and using computer reports as evidence, errors and omissions or malicious intentional acts are possible at each stage of the report-producing process or through nonreal-time program or data modification. It is often not practical to detect or prevent these sufficiently sophisticated intentional acts to alter the reports. Thus, it becomes necessary to take varying degrees of precautions and to invoke the trust of the data processing personnel. Additional confidence in the integrity of the report can be gained by taking the storage medium (tape or disk) to a separate computer center to have its contents printed. Further "independence" can be ensured by verifying that personnel in the new center have no special interest in the work they would be required to do. Throughout the process, independant, trustworthy observers with the skills and knowledge to derermine correct op-

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

erations should observe and supervise all the production steps. 30/

D. STORING AND CARING FOR EVIDENCE

A basic requirement for the admission of evidence is proof that the physical condition of the object is substantially unchanged from its state at the time of seizure. 31/ On the surface, this would not appear to pose any additional problem for computer related evidence than would normally be expected in the handling and storage of regular investigative evidence. However, some types of computer evidence require special care and their storage environments must be controlled, with steps taken to minimize the chance of physical damage from manual handling. Even though most criminal justice agencies normally have acceptable storage facilities for regular types of evidence, these environments may not be suited to computer-related evidence, plus experience in correctly handling computer products may be lacking in their personnel. 32/

Separate types of computer evidence have special needs in their handling and storage. For instance, magnetic tapes and disks should be stored, handled, and transported in hard cover containers. Care should be taken to avoid dropping or squeezing, and no parts of the recording surfaces should be either touched, bent, or creased. The tape reels should be stored vertically in tape storage racks, where room temperatures are between 40 degrees and 90 degrees fahrenheit. Storage life for data retention and recovery is three years. Storage requirements for punch cards and paper tape is similar to that of magnetic tape, except the storage life is indefinite. Special care should be taken to avoid folding, spinning, or knicking edges and tape that might remove paper surfaces should not be used. Computer listings should be stored between binder covers and should not be subjected to strong light. They should

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

be broken into separate pages, unless having them in a continous sheet is important to the case. When storing electronic and mechanical components, it is always wise to consult the manufacturer or owner for special instructions. 33/

Some additional points on the proper handling of computer evidence are also worth mentioning. It is often crucial to a case to specifically identify the location where the physical evidence was acquired. Floor plans, line drawings of the system, and photographs may help in the preparation of the case for court. Lists of the computer evidence and what form it is in - tapes, printouts, cassettes, etc. - are good ideas. Also, the investigator should inscribe computer tapes, disk drives, and print-outs with his personal ID markings. It is appropriate to mark the tapes by writing on the dull side since the first fifteen to twenty feet of tape is "leader" tape and has nothing on it. Identification markings can also be etched on the bottom metal part of a disk pack. Care must be taken in handling these items due to their sensitivity to dust and physical damage. 34/

Finally, to establish that the evidence is substantially unchanged, a complete chain of custody must be readily available. From the initial stages of the search until its completion, careful indexing must be maintained of all the evidence that is seized. 35/

E. PRIVACY AND SECRECY OF EVIDENCE

Issues of personal privacy, trade secrets, or government secrets may sometimes arise since evidence seized in the form of computer media may have data stored that is immaterial to the investigation but that may be confidential to the rightful owner. An obvious consideration would be to ensure that all retrieving and copying on another computer medium contains only that data pertaining to the investigation. In those instances where this is not possible, the investigator should make assurances that any extraneous data will not

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

In those situations where consent to release the information is denied by the owner, sufficient safeguards are available in most jurisdictions to minimize the problem. If necessary, a hearing can be held outside the presence of the jury or even " in camera", to allow the court to either overrule the objection or excise the specific objectionable portions. 36/

III. PROSECUTION AND COMPUTER EVIDENCE

As computer technologies and the means for abusing them have rapidly emerged, they have confronted a criminal justice system which is largely uninformed concerning the technical aspects of computerization. Additionally, this system is bound by traditional legal machinery that is often ineffective against unconventional criminal operations. Difficulties in coping with computer abuse arise because a great deal of the property involved does not neatly fit into the categories of property normally considered as subject to abuse or theft. 37/ It becomes obvious that prosecutors face new and demanding challenges in dealing with their fight against computer crime. Their use of computer evidence is clearly a significant element in the preparation of those difficult cases for prosecution and will be addressed as such in this section of the paper. Certain considerations have been mentioned previously, but merit reconsideration from the prosecutor's viewpoint.

A. FOUNDATIONAL PROBLEMS

Before proffered physical evidence can be admitted into trial evidence, certain foundational facts must be proved by the party seeking admission. When these facts are contrasted with the facts sought to be proved by the evidence, a principal defense avenue of attack is opened to which the prosecutor is particularly vulnerable.

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

of "authentication" which means, in general terms, being able to introduce evidence sufficient enough to sustain a finding that the written statement or document is, in fact, the writing the prosecutor claims it to be. Thus, it becomes necessary to have testimony from someone who can verify that the purported maker of the document (the computer system that generated the item) is the actual maker. Sufficient evidence should be introduced to convince the judge that the proffered item is authentic; however, it is critical at this stage to not claim more than simply the output process, for instance, that the item was generated by such-and-such computer at such-and-such place and time ....nothing more. The prosecutor significantly compounds the authentication problem if an attempt is made to claim that the item reflects a particular configuration or some internal process within the computer. To do so would allow defense to raise valid objections based on the authentication of the specific computer configurations and processes previously mentioned by prosecution. 38/

As stated earlier in the report, for computer media to be admitted as evidence, they must also qualify as business records which are excepted from the application of the Hearsay Rule. 39/ In a 1977 New Jersey case, Monarch Federal Savings and Loan Association v. Genser, the court delineated the requirements necessary in laying the foundation for business records. In Genser, the court held that personal knowledge testimony regarding the information received into the computer is not required, nor is the preparer required to testify. However, testimony is required of a qualified witness who can testify that the computer records were made in the ordinary course of business, were made contemporaneously, what the sources of the information were, and what was the method of preparation. 40/ Although the Genser decision represented a careful and extensive treatment of the problem of admission of

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

decision of the court in one jurisdiction; foundational requirements will vary from state to state. 41/

B. EVIDENTIARY PROBLEMS WITH COMPUTER RECORDS

Computer-generated printed evidence produced to show proof in the courtroom must satisfy the Business Record Exception requirements before being admissable as a hearsay exception. Again, the prosecutor is faced with the burden of showing computer reliability, an area of complex technological issues. His best strategy will hinge upon leading a presumably non-technical court to focus upon the legal issues rather than getting lost in technical matterss. 42/ Although some look upon the computer as no more than a big adding machine, it is impossible to look at the phenomenom of computer crime without considering the varied effects of computers on our legal consciousness. 43/ It is important that the prosecutor be prepared to assist the court with prior and understandable case law dealing with the issue at hand. The best response to defense objections on Business Record Exception issues is to focus on the law, particularly the underlying purposes for the law. 44/

The majority of issues within the past few years regarding computer records and the law of evidence have fallen into three basic categories; (1) admissability of computer printouts; (2) computer printouts as the basis of expert testimony; and (3) discovery matters with regard to computer systems.

Of the above categories, admissibility receives the most attention from the courts. The admissability of computer printouts as evidence depends primarily on whether the data from which the report was generated were entered into the system during the normal course of business. If so, the data record and reports produced subsequently in the regular course of business, or even for trial purposes, may be admissable.

Many of the recent court decisions regarding admissibility of computer

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

printouts have addressed foundational requirements and most allowed the admission into evidence of a computer printout. Typically, in United States v. Farris, the the defendant, convicted of failure to file income tax returns, claimed the court had erred by admitting into evidence the output of a computerized data system. The 7th Circuit Court upheld the admission of the records under 28 U.S.C. #1733(b), which allows admission of authorized copies of documents of United States departments as if they were originals.

A 1976 decision bears on issues raised by computer records being used as the basis for expert testimony. In Perma Research and Development v. Singer Co, a breach of contracts civil suit, the defendant objected to the use of the results of computer simulations as a basis for the plaintiffs expert testimony. Although the court admitted that it would have been better for the plaintiff's counsel to have delivered to defense, prior to trial, the details of the underlying data and theorems so as to avoid discussion of their technical nature during trial, it did not charge the trial judge, however, with abuse of discretion for allowing the expert's testimony regarding the results of the computer simulation.

In United States v. Liebert, a discovery issue was raised as to whether pretrial discovery may be used by defense to secure extrinsic evidence to impeach the reliability of a computer printout. Again, the defendant in this case was charged for failure to file tax returns. The IRS computers had no record of the defendant's filing and the defendant requested that his computer expert have access to the IRS Service Center to test the reliability of the IRS data process system; the request was granted. The defendant then requested, for discovery purposes, records of any notices sent to persons stating that the IRS had failed to receive their returns. When the court granted the defendant's request as to a portion of the list of non-filers, the government refused to comply with the court order and the defendant's case was dismissed. On

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

appeal, the dismissal was reversed and the appellate court held that supplying the list requested by the defendant would be unreasonable because of the infringement of the right of privacy of those persons on the list. The IRS's willingness to make available all documents regarding their procedures, operations, and electronic data processing system to discover nonfilers, and their willingness to allow their expert witness to be deposed, was held sufficient to provide the defendant with an opportunity to question the accuracy of the system. 45/

C. PRACTICAL RECOMMENDATIONS

Computer crimes are difficult cases to develop and solve and sometimes require many more resources than most organizations have at their disposal. 46/ Often, legal problems are unavoidable. However, adherence to good investgative methodology, and thorough planning for trial will help the case work flow smoothly. 47/ The practical recommendations that follow, while certainly no panacea, are proven good advice and will enhance the prosecutor's chances of success.

Expert witnesses are often the keys to the admission of evidence in computer criminal trials. Since computer technologists have little or no experience as expert witnesses, they must be carefully "coached" prior to their testimony. It is crucial to keep the computer expert in control and force him to answer questions in court in as few words as possible. One means of achieving thisis to ensure the questions themselves are well formulated so as to elicit brief responses. Remember that good witnesses are those who know what they are talking about and can show that the method of generating the evidence is valid. 48/

Prosecutors should remember that the most likely image that the judge and jury have of computer technology is what they last read on the front page

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

of events. It is therefore important to make the case as basic, simple,and free from computer technology and terminology as possible, explaining only those circumstances necessary to present the case. If possible, rely on paper records if they exist rather than introducing computer-generated records. Do not personify or anthromorphize computers in presentations; rather, treat them strictly as inanimate objects, machines, subject to use and manipulation by people. The bottom line, Keep It Simple! 49/

Prosecutors should also attempt to determine the trial judges degree of knowledge and attitude towards computer technology and gear their presentation accordingly. For example, Judge Van Graafeiland of the United States Second Circuit Court of Appeals has said, "As one of the many who have received computerized bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of Holy Writ." 50/ It is, therefore, important to present, and make common knowledge, a convincing argument depicting computerized record keeping as rapidly becoming a normal procedure in the business world.

IV. CONCLUSION

In this paper we have examined several different aspects of evidence in computer crime cases, and the criticality of evidentiary issues to the successful prosecution of computer criminals. Computer crime continues to grow by leaps and bounds, making it imperative that investigators and prosecutors become ever more reliant upon improving their training and skills in this area. In 1980, experts at the Federal Bureau of Investigation estimated that only one of 22,000 computer criminals goes to jail. Further, they estimated that only 1% of all computer crimes is detected, only 14% of that is reported, and only 3% of those cases ever result in jail sentences; clearly leaving

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

In addressing the different investigative evidentiary considerations, as well as the role of computer evidence in criminal prosecution, we have seen the value of being properly prepared for the investigation, from the initial search to the final court trial, and for careful adherence to established legal principles. We have also observed the apparent need for better training for both investigators and prosecutors in the area of computer crime evidence, as well as the need to better utilize the services and advice of those who are most knowledgeable of computer technology and operations.

In response to a survey by the American Bar Association Task Force on Computer Crime, an executive for a consumer reporting agency appropriately stated: " The most difficult task at present is to educate government so as to make them aware of the computer problem. Law enforcement agencies are not familiar enough with computers and the losses that can occur to properly conduct an investigation and prosecute the perpetrators." 52/ A step in the right direction is the FBI Academy's development of a computer crime course to assist investigators and prosecutors in gaining a better understanding of the technical and legal aspects of computer crime. 53/ Combining the expectation of hard work, friendly patience, access to the FBI computer, and a variety of motivational techniques, the Academy staff has proceeded with efficiency to create a core of law enforcement personnel with a expanded knowledge of computer crime. With this knowledge comes the ability to communicate more directly and meaningfully with the computer experts necessary at the various stages of the investigation and subsequent trial. 54/

Throughout the investigative process, the investigator should be willing to actively seek out the persons who are most knowledgeable of the particular computer regimen in question, to assist in identifying and explaining what

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

organization has a security specialist, he can be of great assistance in conducting the investigation. He will likely be very knowledgeable of the computer system and his records could provide significant amounts of evidence that might be used in criminal trial, particularly since they may be exceptions to hearsay evidence rules due to their being produced in the normal course of business. 55/

As Sen. Paul Tribile (R - Va), the leading sponsor of the Computer Fraud and Abuse Act, stated: "It is time to dispel the notion that computer crime is a game or a challenge to be overcome. The fact is, the computer criminal is a law breaker just like any other and deserves to be treated as such." 56/ Understanding and adhering to the proper evidentiary principles in computer crime investigations will undoubtedly assist in that effort.

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

FOOTNOTES

1/ House of Representatives Report 99-753, 99th Congress, 2d Session, Computer Security Act of 1986, August 6, 1986, p.1.

2/ House of Representatives Report 99-894, 98th Congress, 2d Session, Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, July 24, 1984,p.9.

3/ National Criminal Justice Information and Statistics Service, Law Enforcement Assistance Administration, U.S. Department of Justice, Computer Crime-Criminal Justice Resource Manual, (Washington, D.C.: Government Offices, 1979), p.100.

4/ Donn Parker, Fighting Computer Crime, (New York: Charles Scribner's Sons, 1983), p.x .

5/ J.J. Bloombecker, "New Federal Law Bolsters Computer Security Efforts", Computerworld, October 27, 1986,pp. 64-66.

6/ John Sauls, "Raiding the Computer Room, Fourth Amendment Considerations (Conclusion)," FBI Law Enforcement Bulletin, June 1986,pp. 24-30.

7/ John Sauls, "Raiding the Computer Room, Fourth Amendment Considerations (Part I)", FBI Law Enforcement Bulletin, May 1986, pp. 25-30.

8/ Task Force On Computer Crime, Section of Criminal Justice, American Bar Association, Report on Computer Crime, (Washington, D.C.: Government Printing Office, 1984), pp. II-8.

9/ National Criminal Justice Information and Statistics Service...., p.100.

10/ National Criminal Justice Information and Statistics Service...., p. 100.

11/ Sauls (Part I), p. 26.

12/ J.J.Becker, The Investigation of Computer Crime, An Operational Guide to White Collar Crime Enforcement, (Washington, D.C.: Government Printing Office, April 1980), p. 24.

13/ J.J. Becker, "Programmed For Crime", Los Angeles Lawyer, November 1979, pp. 16-31.

14/ Sauls (Conclusion), pp. 24-25.

15/ Sauls (Part I), pp. 26-29.

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

16/ National Criminal Justice Information and Statistics Service, p. 27.

17/ Sauls (Conclusion), p. 27.

18/ National Criminal Justice Information and Statistics Service...., p. 100.

19/ Becker, The Investigation of Computer Crime...., p. 19.

20/ National Criminal Justice Information and Statistics Service....,p.101.

21/ Becker, The Investigation of Computer Crime...., p. 14.

22/ National Criminal Justice Information and Statistics Service...., p. 101.

23/ National Criminal Justice Information and Statistics Service...., p.10.

24/ National Criminal Justice Information and Statistics Service...., p.102.

25/ Becker, The Investigation of Computer Crime...., p. 25.

26/ Sauls (Conclusion), p. 29.

27/ James Vergari, "Evidential Value and Acceptability of Computer Digital - Image Printouts", Rutgers Computers and Technology Law Journal, Vol 9, (1984), p. 346.

28/ Chi K.L. Lam, "Can Computer Output Be Evidence?", The EDP Auditor, Journal of the Auditor's Foundation, Fall 1982, p.43.

29/ Vergari, p.347.

30/ National Criminal Justice Information andStatistics Servece...., p.110.

31/ Becker, The Investigation of Computer Crime...., p. 27.

32/ National Criminal Justice Information and Statistics Service...., p. 111.

33/ Bruce Goldstein, A Pocket Guide to Computer Crime Investigation, (Madison, Wisconsin: Assets Protection, 1981), pp. 17-18.

34/ Goldstein, p. 15.

35/ Becker, The Investigation of Computer Crime...., p.112.

36/ National Criminal Justice Information and Statistics Service...., p. 112.

37/ House of Representatives Report 99-894...p. 9.

38/ NationalCriminal Justice Information and Statistics Service...., p. 113.

39/ Becker, The Investigation of Computer Crime...., p.30.

40/ National Criminal Justice Information and Statistics Service...., p.121.

41/ Becker, The Investigation of Computer Crime...., p. 30.

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6

43/ Becker, "Programmed For Crime"..., p.66.

44/ National Criminal Justice Information and Statistics Service..., p. 116.

45/ National Criminal Justice Information and Statistics Service...., p.124.

46/ Goldstein, p.5.

47/ Lam, p. 57.

48/ National Criminal Justice Information and Statistics Service...., p. 124.

49/ National Criminal Justice Information and Statistics Service...., p.125.

50/ Lam, p.52.

51/ Becker, The Investigation of Computer Crime...., p.6.

52/ Task Force on Computer Crime...., p.5.

53/ Glenn McLoughlin, "Computer Crime and Security Updated", Issue Brief, Congressional Research Service, Library of Congress, September 15, 1986, p. 9.

54/ J.J. Becker, "Computer Crime Fighters.... Go To Boot Camp At FBI Academy", Security World, September 1978, pp. 30-31.

55/ National Criminal Justice Service Information and Statistics Service..., p. 102.

56/ Kevin Power, "Congress Approves Law to Combat Computer Crime", CCH, October 24, 1986, p. 5.

Declassified in Part - Sanitized Copy Approved for Release 2014/01/15 : CIA-RDP89G00643R000300030005-6